

U.S. General Services Administration (GSA)

PRESIDENTIAL TRANSITION KEY ISSUES INFORMATION PAPER

SUBJECT: Strengthening Federal Cybersecurity

1. BACKGROUND:

General Background:

- In the Fiscal Year 2017 Budget, the President requested an additional \$19 billion for improving the nation's cybersecurity (a 35% increase from the previous budget). Additionally, the President launched the Cybersecurity National Action Plan (CNAP), a comprehensive set of initiatives that directs the Federal Government to take many immediate steps to improve Federal cybersecurity, while fostering the conditions required for long-term improvements in our approach to cybersecurity across the Federal Government, the private sector, and our personal lives.
- Many of the initiatives detailed in the CNAP request that GSA assume a primary leadership role, especially regarding the modernization of legacy IT throughout agencies and to improving the effectiveness and efficiency of cybersecurity acquisition.

b. Issues:

- GSA is tasked with sustaining many of the highest priority CNAP initiatives going forward, often without additional funding or other resources.
- GSA's previous efforts to help other agencies procure and implement stronger, more secure systems and technologies will only continue with committed executive-level leadership in the next Administration.

2. SCOPE AND EFFECT:

a. Impact on GSA's Customers:

- Through new acquisition vehicles, such as the [HACS SINs](#) on IT Schedule 70, agencies can now more easily acquire essential cybersecurity services through well-vetted vendors and ensure compliance with Department of Homeland Security assessment methodology. Some of the benefits include:
 - i. Ease of ordering. Quick and easy access to the right industry partners, allowing customers to make the most use of their valuable time.
 - ii. GSA Schedule pricing is pre-determined by GSA to be fair and reasonable
 - iii. Up-to-date, FAR-compliant acquisition vehicles that help minimize risks, and
 - iv. Save time & money: Schedule orders average 15 days while open-market procurement averages 268 days.
- Capabilities provided by the HACS SINs help agencies meet FISMA requirements, as well as comparable evaluations that mirror DHS's High Value Asset (HVA) assessments. Services that can be procured from the HACS SINs include:

- i. Penetration Testing
- ii. Incident Response
- iii. Cyber Hunt
- iv. Risk and Vulnerability Assessment

- Through a partnership between DHS and GSA, new capabilities will be added to the HACS SINS as the HVA Assessment process, and the findings produced by the process, are leveraged to define new requirements for new service offerings.

b. Impact on the Private Sector and State & Local Governments:

- Many new, small businesses have joined the HAC SINS and are now providing their services to the Government.
- State, local, tribal, and territorial governments can procure any services available on the HACS SINS - and, since many of their systems are connected with or communicate to federal systems, their participation is strongly encouraged.

3. ACTION(S) PLANNED OR REQUIRED:

- GSA and DHS will continue to identify agencies and agency systems that can leverage the HACS SINS for their testing and remediation needs, and will continue to personally assist such agency customers in utilizing the HACS SINS to conduct "HVA-like assessments"
- GSA will continue to grow and matures other CNAP offerings for which is has primary responsibility
 - i. Developing a Bug Bounty program and vehicle to assist agencies in testing and remediating its surface level vulnerabilities
 - ii. Improving email and collaboration tool rationalization and adoption among agencies
 - iii. Continuing to mature and improve the offerings, tools, and services available under the Continuous Diagnostics and Mitigation procurement vehicle
 - iv. Acceleration PIV adoption and use to increase the amount and effectiveness of two-factor authentication across government

4. KEY STAKEHOLDER INTEREST:

- Office of Management and Budget (especially the Office of the Federal Chief Information Officer)
- National Security Council
- Department of Homeland Security

- All Federal CFO Act Agencies (who are required to participate in the CNAP)
- Small Agencies, and State/Local/Tribal/Territorial Governments

5. FISCAL YEAR 2017/2018 BUDGET IMPACT:

- No additional appropriated dollars has been requested to administer the several high profile activities GSA administers that improve Federal cybersecurity